UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

United States of America,

Plaintiff,

v.

Case No.: 1:19-cr-00089

Judge Michael R. Barrett

Abeth Vivas Laynes,

Defendant.

OPINION & ORDER

This matter is before the Court on Defendant Abeth Vivas Laynes' Motion to Suppress Evidence (Doc. 33), as supplemented (Docs. 36, 43). For the reasons that follow, Defendant's Motion will be GRANTED.

I. BACKGROUND

A. Pre-hearing arguments

Defendant originally was indicted on July 31, 2019 on three counts of sexual exploitation of children in violation of 18 U.S.C. §§ 2251 (a) and (e), with a forfeiture allegation. (Doc. 15). The "visual depictions" Defendant was accused of producing were videos. (*Id.* at PageID 35). Defendant filed his motion on January 31, 2020 (Doc. 33) and initially argued that the evidence seized from his iPhone must be suppressed because, after *Riley v. California*, 573 U.S. 373 (2014), all searches of cellular phones at the border require a warrant. Because no warrant was obtained before the border patrol searched his iPhone and located child pornography on it, the search was improper. Defendant argued alternatively that, after *Riley*, a search of a cellular phone

at the border requires reasonable suspicion at a minimum. And because reasonable suspicion was lacking, the search was improper under the Fourth Amendment.

The United States filed its memorandum in opposition to Defendant's initial motion on February 19, 2020. (Doc. 34). It argued that neither a warrant nor probable cause—or even reasonable suspicion—was needed to manually examine Defendant's iPhone pursuant to a routine border search. Alternately, if the Court were to find a violation of the Fourth Amendment, the good-faith exception applies because the border patrol officers reasonably relied on the existing precedent at the time regarding the border-search exception to the warrant requirement.

B. The March 2, 2020 hearing

Three officers from U.S. Customs and Border Protection ("CBP") and a special agent from Homeland Security Investigations ("HSI") testified at the March 2, 2020 hearing.

Defendant, a Mexican citizen and Lawful Permanent Resident ("LPR", also known as a "green card holder") of the United States, returned from Mexico City to his home in the Greater Cincinnati area on July 4, 2019. His flight required a change at Detroit Metropolitan Airport ("DTW"), where he entered the United States from Mexico.

That evening, CBPO Satwinder Sidhu was stationed in a "primary" booth, the first stop for an individual coming off an international flight. Each passenger's name is run through the Treasury Enforcement Communications System known as "TECS." Defendant was flagged as an LPR, and as such, CBPO Sidhu was required to capture his fingerprints. After doing so, the program then instructed her to refer Defendant to Passport Control Secondary. As she explained, "[f]rom my experience, biometric watch

list, somebody – any individual would hit on that list if that individual's fingerprints FIN number was promoted to that watch list by another law enforcement agency for – could be criminal issues, immigration issue, could be any of the – one of the many reasons." (Hearing Tr., Doc. 42 at PageID 173 (15:13–18)).

CBPO Michael Beard, assigned to the Admissibility Enforcement Unit and present at Passport Control Secondary, saw Defendant next. He explained that Defendant would have been placed on the watch list if, as a green card holder, he had committed a crime involving "moral turpitude." If so, that could possibly trigger a "Notice to Appear" ("NTA") before an immigration judge to determine whether Defendant should be removed from the United States. (*Id.* at PageID 179 (21:1–19)). Specific to Defendant, his criminal record reflected a juvenile arrest—when he was approximately eleven years-old—for first degree sexual assault of a minor, and arrests as an adult for driving while under the influence in both Ohio and Wisconsin. (Gov't Exh. 6 at 2). Because he was "so young" when he was arrested for sexual assault, CBP determined there was no need for him to appear before an immigration judge. (Hearing Tr., Doc. 42 at PageID 181 (23:4–11)). While that decision was being made, however, CBPO Beard decided to examine Defendant's cell phone.

CBP has a specific and detailed policy that governs the search of electronic devices, including cell phones. (Gov't Exh. 3). According to CBPO Beard, "[w]hen we look through a phone, we make sure that it's in airplane mode so that it's not attached to any cloud or web-based information before we do anything." (Hearing Tr., Doc. 42 at PageID 182 (24:1–3)[1]; *see* Gov't Exh. 3[2] at 4 (§ 5.1.2) ("The border search will include

[1] *Cf.* (Hearing Tr., Doc. 42 at PageID 199 (41:14–24)).
[2] Government Exhibit 3 was admitted post-hearing. (*See* 04/21/2020 Minute Entry).

an examination of only the information that is resident upon the device and accessible through the device's operating system or through other software, tools, or applications. Officers may not intentionally use the device to access information that is solely stored remotely. To avoid retrieving or accessing information stored remotely and not otherwise present on the device, Officers will either request that the traveler disable connectivity to any network (e.g., **by placing the device in airplane mode**), or, where warranted by national security, law enforcement, officer safety, or other operational considerations, Officers will themselves disable network connectivity.") (emphasis added)). Specific to Defendant's iPhone, and purportedly in compliance with border-search policy, Beard testified, "[a]fter placing it in airplane mode and recording the [IMEI, serial number, and model number] information, I opened up Google Photos." (Hearing Tr., Doc. 42 at PageID 183 (25:23–24)). The "first thing" Beard saw on Google Photos was a video of "a toddler or a younger boy having sex with an adult woman." (*Id.* at PageID 183–84 (25:25–26:10)).[3] After finding this video of child pornography, Beard handed the phone to his colleague, CBPO Patrick Mengel, and, as is standard practice, Mengel contacted HSI Special Agent George Melvin. Melvin told Mengel to keep looking for additional child pornography.

[3] CBPO Beard confirmed on cross-examination that he looked in the Google Photos application, not in the iPhone photos:

> Q. All right. This is an iPhone, so did it have an app for Google Photos, or why were you in Google Photos?
> A. It would have been an app.
> Q. Okay. Do iPhones have their own – are you familiar with iPhones from your work?
> A. Somewhat, yes.
> Q. Do they have their own program for pictures?
> A. They do.
> Q. Did you look for an iPhone app for pictures?
> A. The first one I noticed was the Google app, so that's the one I went into.

(Hearing Tr., Doc. 42 at PageID 196 (38:8–18)).

Following Agent Melvin's instruction, CBPO Mengel looked at "Photos, Email, WhatsApp, and Notes" in Defendant's iPhone and, in the camera roll of Photos, found three Live Photos[4] that depicted child pornography. Specifically, the photos "looked like a vagina of a small child in an adult's hand." (*Id.* at PageID 208 (50:18–20)). The geolocation coordinates of those Live Photos matched the address on Defendant's driver's license. (*Id.* at PageID 209 (51:2–21) ("If you swipe up on a photo on an iPhone if the geotag is on, then you can get the address of where the photo was taken.")). Mengel did not recall whether he checked to see if the phone was in airplane mode during his search, presuming that CBPO Beard had already done so. (*Id.* at PageID 210–11 (52:10–53:5) ("I normally don't check to verify it's in airplane mode.")).

When Agent Melvin arrived, he noticed that the iPhone CBPO Mengel gave him was actually *not* in airplane mode. (*Id.* at PageID 220 (62:13–18)). He then put it in airplane mode and viewed the Live Photos about which Mengel testified. (*Id.* at PageID 220–21 (62:19–63:1)). Back at his office, Melvin was unable to view a video that one of the officers showed him upon arrival. He then took the device *out* of airplane mode and that video played. (*Id.* at PageID 224 (66:5–19) ("[I]t depicted a younger girl that could have been in a compromising position."); 230 (72:4–12) ("[I]t involved a young girl giving fellatio.")).

Ultimately, Defendant was admitted into the United States the evening of July 4, 2019, but without his iPhone.

[4] Asked to explain a "Live Photo," CBPO Mengel stated: "With an iPhone, if you take a photo and the Live Photo mode is on, if you press the photo, it will play, like, a short, two-second clip of the photograph. So it turns it into, like, a two-second video. (Hearing Tr., Doc. 42 at PageID 208–09 (50:22–51:1)).

C. Post-hearing supplemental arguments

In his post-hearing brief filed on March 20, 2020 (Doc. 36), Defendant argues that the evidence of child pornography seized from his iPhone should be suppressed because CBPO Beard failed to place it in airplane mode, as required by CBP policy, rendering the border-search doctrine inapplicable. He also reprises his argument that *Riley* requires either a warrant or reasonable suspicion to search a cell phone at the border, and he maintains that the search of the iPhone cannot be saved by good faith. Thus, the video found by CBPO Beard, as well as all other evidence of child pornography, must be suppressed as the fruit of the poisonous tree.

The United States responds (Doc. 37, filed 04/10/2020) that any failure to place Defendant's iPhone in airplane mode, even in violation of agency policy, does not vitiate an otherwise valid border search. The manual (as opposed to forensic) search of Defendant's iPhone by the CBP officers was routine and, as such, did not require a warrant or reasonable suspicion. Further, any failure to place the device in airplane mode, which may have resulted in viewing remotely-stored images and videos, was a reasonable mistake not warranting suppression. And, in any event, the inevitable discovery doctrine would apply to the searches of remotely-stored images and videos.

D. Superseding Indictment

On June 3, 2020, the United States filed a superseding indictment against Defendant. (Doc. 38). It is identical to the original indictment, except that the "visual depictions" Defendant is accused of producing are images rather than videos. (*Id.* at PageID 147).

E. The June 10, 2020 hearing

The hearing on Defendant's Motion to Suppress resumed on June 10, 2020, with HSI Special Agent Christopher Wallace testifying. Agent Wallace conducted a forensic examination of Defendant's iPhone, which, through the use of metadata[5], allowed him to determine when and where certain child pornography images were "captured" on the device. As part of that examination, he created summaries of each image or video found on the iPhone. One such summary was an image with a "capture time" of "12/28/2017 1:05:42 PM" and a "Created" and "Modified" date of "2019-06-13." (Gov't Exh. 7A).[6] June 13, 2019 unmistakably predates July 4, 2019, the date Defendant's iPhone was searched at the Detroit border, proving that this image was then "resident" on Defendant's device. Further, this image was associated with a latitude/longitude location that corresponded with a residential address (9881 Loralinda Drive) previously linked to Defendant. Two other summaries were introduced. These images had "capture times" of "12/28/2017 1:05:48 PM" and "12/28/2017 1:05:52 PM," respectively, along with the same "Created and Modified" date of "2019-06-13," and were likewise associated with the Loralinda Drive address. (Gov't Exhs. 8A, 9A).

Agent Wallace confirmed on cross-examination that an iPhone has its own application for photos called "Photos." This is commonly referred to as the iPhone's "camera roll." The iPhone Photos application is different from the Google Photos application that CBPO Beard looked at when he searched Defendant's iPhone. Wallace acknowledged that Google Photos uses cloud storage for videos and pictures and that

[5] Agent Wallace testified that metadata is "data about data." *See also* https://www.merriam-webster.com/dictionary/metadata ("data that provides information about other data") (last visited July 6, 2020).
[6] This image also lists "created and modified" dates "2019-06-13 02:31:18"

Defendant's iPhone was accessing the cloud at the time of the search. He also testified that he could not determine whether the video that CBPO Beard viewed was resident on the phone or whether it was viewed in the cloud. Finally, Wallace stated that there are several "clearly visible" indictors that would tell a person whether an iPhone is in airplane mode, including a picture of an airplane on the home screen.

F. Concluding arguments following the June 10, 2020 hearing and preparation of the March 2, 2020 hearing transcript

The Court permitted one further round of briefing following the June 10, 2020 hearing and preparation of the March 2, 2020 hearing transcript. (Docs. 43–45). As established during a status conference by telephone on June 30, 2020, the record in this matter was closed with the filing of Defendant's reply on July 22, 2020. (*See* 06/30/2020 Minute Entry).

Defendant emphasizes that, because his iPhone was not in airplane mode when CBPO Beard searched it, the phone was accessing remote, or cloud, storage. Google Photos, the sole application searched by Beard, uses cloud storage for videos. Beard immediately passed the iPhone to CBPO Mengel. Neither Mengel nor Agent Melvin would have searched the iPhone if Beard had not seen the video of child pornography on Google Photos. Agent Wallace, having conducted a forensic search, could not determine whether that video was resident on the phone before the search or was being viewed by CBPO Beard in the cloud. Based on the United States' concession that the CBP's border-search authority does not extend to searches of remotely-stored information under *Riley*, all evidence of child pornography obtained during these various searches must be suppressed as the fruit of the poisonous tree. Moreover, the inevitable discovery rule cannot apply, because the searches of his iPhone were

"indisputably" the direct result of the unlawful search by CBPO Beard. (Doc. 43 at PageID 250). Agent Wallace's testimony—that there were pictures depicting child pornography resident on the phone as of December 28, 2017 that the CBP *could have viewed* in the Photos camera roll while the iPhone was in airplane mode—fails to satisfy the Government's burden. "Could have" and "inevitably would have" are simply not the same.

The United States concedes that there was an unlawful search of "remotely stored information" on Defendant's iPhone, but counters that the search generally was made pursuant to a lawful border search. (Doc. 44 at PageID 255). The "remote based child pornography" should not be suppressed because "it was the byproduct of a reasonable mistake" by CBP—that is, believing that the iPhone was in airplane mode and thus not accessing the cloud. Further, because there was child pornography resident on the iPhone, HSI would have requested follow-up search warrants vis-à-vis Defendant's remote storage accounts and inevitably discovered the images and videos that Defendant seeks to suppress. With no predicate unlawful search, the fruit-of-the-poisonous-tree doctrine is inapplicable. But setting aside whether the remotely-accessed child pornography is properly suppressed, the CBP officers inevitably would have discovered the child pornography images resident on the phone. Had Officer Beard not been able to access the Google Photos application because the iPhone was in airplane mode, he simply would have searched elsewhere on the phone. Finally, and presuming the Court were to find a Fourth Amendment violation, the CBP officers acted in objective good faith such that suppression would not have a deterrent effect.

II. ANALYSIS

As noted by the United States, the Government's authority "to conduct routine searches and seizures at the border, without probable cause or a warrant, . . . to prevent the introduction of contraband" has existed "[s]ince the founding of our Republic." *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985).[7] Thus, routine searches of travelers and their belongings "are not subject to any requirement of reasonable suspicion, probable cause, or warrant[.]" *Id.* at 538 (footnote omitted). This broad exception to the Fourth Amendment is made because the Government's interest in preventing the entry of "unwanted person and effects is at its zenith at the international border." *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004). Border-search authority extends to "functional equivalents" of the border, including airports—such as DTW—where international flights land. *United States v. Stewart*, 729 F.3d 517, 524 (6th Cir. 2013).

A. As a General Matter, *Riley* Does Not Require Either a Warrant or Reasonable Suspicion for a Routine Border Search of an iPhone

In *Riley v. California*, the Supreme Court addressed whether the Government is required to obtain a search warrant before conducting a search of a cell phone during a search incident to a lawful arrest. 573 U.S. 373 (2014). Answering yes, the Court observed that cell phones differ substantially from other personal items subject to search upon arrest:

> The United States asserts that a search of all data stored on a cell phone is "materially indistinguishable" from searches of these sorts of physical items. . . . That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies

[7] It is a criminal offense to transport child pornography into the United States. *See* 18 U.S.C. § 2252(a)(1).

> lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items but any extension of that reasoning to digital data has to rest on its own bottom.

Id. at 393. And because the Supreme Court has specifically likened a search incident to arrest to a border search, Defendant urges this Court to hold that a warrant is required to search a cell phone in the latter instance also. *See United States v. Ramsey*, 431 U.S. 606, 621 (1977) ("[The 'border search' exception] is a longstanding, historically recognized exception to the Fourth Amendment's general principle that a warrant be obtained, and in this respect is like the similar 'search incident to lawful arrest' exception[.]").

Defendant relies on *United States v. Aigbekaen*, 943 F.3d 713 (4th Cir. 2019) for the proposition that the border-search doctrine does not justify a warrantless search of a cell phone at the border. As the Government points out, however, the facts of *Aigbekaen* are inapposite. There, the defendant was suspected of being involved in domestic sex trafficking. *Id.* at 717. Upon his return to the United States and at the *advance* request of HSI, CBP seized defendant's laptop, iPhone, and iPod at the airport and HSI thereafter conducted warrantless forensic searches of the data on all three devices. *Id.* These searches were found unconstitutional because

> the reasonableness of requiring law enforcement to secure a warrant before conducting an intrusive forensic search of a traveler's digital device, **solely to seek evidence of crimes with no transnational component**, is readily apparent. **By the time Aigbekaen arrived at the airport with his devices, and prior to any searches of those devices, HSI agents had probable cause to believe that Aigbekaen's laptop, at least, contained evidence of domestic sex trafficking.** Indeed, in August of 2015,

> HSI secured warrants to search both the MacBook Pro and the iPhone, relying almost exclusively on evidence that was in agents' possession before Aigbekaen arrive at the airport in May. **Given the information in its possession at the time, it is only reasonable to expect the Government to have procured these warrants prior to the May searches.**

Id. at 722 (emphasis added) (footnote omitted). Here, in contrast, HSI did not use the border-search doctrine as a ruse to conduct a warrantless forensic search of Defendant Laynes' iPhone. Moreover, citing *Ramsey*, the Fourth Circuit specifically reserved ruling on the question Defendant Laynes presents. *Id.* at 723 ("Because Aigbekaen does not challenge any *routine* border searches, we need not decide whether or how the interests that underpin the border search exception constrain, in practice, the Government's broad and historic authority to conduct suspicionless searches of individuals and their effects at the border.") (emphasis in original)).

On the other hand, the Ninth Circuit has determined that, post-*Riley*, border officials may still conduct suspicionless manual searches of cell phones. *United States v. Cano*, 934 F.3d 1002, 1014–16 (9th Cir. 2019).[8] This Court agrees. The difference in context between the border-search exception and the search-incident-to-arrest exception is "critical." *Id.* at 1015. The Fourth Amendment's balance is "struck much more favorably to the Government" considering the Government's duty to protect the integrity of the border measured against the traveler's decreased expectation of privacy. *Id.* (citing *Montoya de Hernandez*, 473 U.S. at 538–40)).

Defendant alternately argues that *Riley* requires at least reasonable suspicion before manually searching a cellular phone at the border, and, in this instance, there

[8] The Sixth Circuit has yet to address the issue of the border search of an electronic device (or cellular phone specifically) since *Riley* was decided.

was none.[9] But the cases Defendant cites relate to *forensic* examination of digital devices, not a preliminary manual search. *See Cano*, 934 F.3d at 1016 ("the forensic examination of a cell phone [at the border] requires a showing of reasonable suspicion");[10] *United States v. Kolsuz*, 890 F.3d 133, 144 (4th Cir. 2018) (post-*Riley*, "a forensic border search of a [cell] phone must be treated as nonroutine, permissible only on a showing of individualized suspicion"); *United States v. Kim*, 103 F. Supp. 3d 32, 59 (D.D.C. 2015) (search of laptop unreasonable because it was "aided by specialized forensic software, for a period of unlimited duration and an examination of unlimited scope, for the purpose of gathering evidence in a pre-existing investigation, [and] was supported by so little suspicion of ongoing or imminent criminal activity, and was so invasive of [the defendant's] privacy and so disconnected from not only the considerations underlying the breadth of the [G]overnment's authority to search at the border, but also the border itself[.]"); *United States v. Saboonchi*, 48 F. Supp. 3d 815, 819–20 (D. Md. 2014) ("An invasive [meaning forensic] and warrantless border search may occur on no more than reasonable suspicion[. . .] and nothing in *Riley* appears to have changed that.") Further, as Defendant acknowledges, the Eleventh Circuit has held, post-*Riley*, that *no* level of suspicion is required for a border search of an electronic device, manual *or* forensic. *United States v. Touset*, 890 F.3d 1227, 1233 (11th Cir. 2018) ("We see no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property.").

[9] The Government does not argue that reasonable suspicion existed, only that it was not needed.
[10] *Cano* relies on a pre-*Riley* decision, *United States v. Cotterman*, 709 F.3d 952, 968 (9th Cir. 2013), in which the Ninth Circuit held that reasonable suspicion was required for the forensic examination of a laptop computer at the border.

Even if this Court were to hold that either a warrant or reasonable suspicion was required to manually search Defendant Laynes' iPhone, which it does not, the good-faith exception would nevertheless apply. No case post-*Riley* has limited the Government's authority to conduct suspicionless manual searches of electronic devices at the international border. Thus, the CPB officers reasonably relied on existing precedent in July 2019 when they commenced their preliminary manual search of Defendant's iPhone, and exclusion of its contents on this basis would not be an appropriate remedy. *Davis v. United States*, 564 U.S. 229, 236–37 (2011) (exclusionary rule's "sole purpose" is "to deter **future** Fourth Amendment violations") (emphasis added). *See Aigbekaen*, 943 F.3d at 725 ("Given the uniform body of precedent that permitted warrantless [forensic] searches [of electronic devices] at the border in May of 2015, we cannot help but conclude that the good-faith exception applies here.").

B. CBP's Failure to Follow Its Own Procedures, However, Warrants Suppression of the Child Pornography Found on Defendant's iPhone

Approximately eighteen months prior to the search of Defendant's iPhone, CBP published an updated Privacy Impact Assessment ("PIA") regarding its policy and procedures for conducting searches of electronic devices pursuant to its border search authority. *See* DHS/CBP/PIA-008(a) Border Searches of Electronic Devices (January 4, 2018), available at www.dhs.gov/publication/border-searches-electronic-devices (Gov. Exh. 5).[11] The PIA distinguishes between "basic" and "advanced" searches, which seems to largely equate to the "manual" and "forensic" searches as described in the caselaw previously discussed. "A CBP Officer may perform a basic search of the electronic device in front of the passenger with or without suspicion." (*Id.* at 6). "This

[11] This PIA also was attached to Defendant's original Motion to Suppress.

search may reveal information that is **resident upon the device** and would ordinarily be visible by scrolling through the phone manually (including contact lists, call logs, calendar entries, text messages, pictures, videos, and audio files). (*Id.* (emphasis added)). An "advanced" search is defined as "any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents." (*Id.*). Pertinent here, and in a subsection titled, "Restriction on CBP Access to Information in the 'Cloud'," the PIA states:

> In the 2018 Directive, CBP has formally clarified the scope of the information in accesses when conducting border searches of electronic devices. The updated policy clarifies that a border search includes an examination of only the information that is **resident upon the device** and accessible through the device's operating system or through other software, tools, or applications. For both basic and advanced searches, Officers may not intentionally use the device to access information that is solely stored remotely. **Prior to beginning a basic or advanced search**, CBP Officers **must** take steps to **ensure** that a device **is not connected to any network**. **To avoid retrieving or accessing information stored remotely and not otherwise present on the device, Officers will either request that the traveler disable connectivity to any network (e.g., by placing the device in airplane mode), or**, where warranted by national security, law enforcement, Officer safety, or other operational considerations, Officers **will themselves disable network connectivity**. Officers also take care to ensure, throughout the course of a border search, that they do not take actions that would make any changes to the contents of the device.

(*Id.* at Page 8 (footnotes omitted) (emphasis added)).

Based on the hearing testimony and exhibits, including the PIA just discussed, there is no dispute that CBP policy requires that a cell phone be put in airplane mode before it is searched. CBPO Beard put it succinctly: "[S]tep one" is "always get that device in airplane mode[.]" (Hearing Tr., Doc. 42 at PageID 184 (26:23–25)). Yet

Beard, a veteran officer at DTW since 2006 who has examined some 100 electronic devices, apparently failed do so. True, Beard testified on cross-examination that "[t]he officer that I would have handed it to, which would have been Officer Mengel, I gave it to him in airplane mode." (*Id.* at PageID 195 (37:23–24)). But Mengel did not check whether the phone was disabled, and, as a practice, would not have checked. Why? Because he relied on the fact "that it should have been placed in airplane mode at the start." (*Id.* at PageID 210 (52:19–25)). Yet Agent Melvin noticed *immediately* that Defendant's iPhone was not in airplane mode. And Agent Wallace testified to the "clearly visible" indicators that would show whether an iPhone is in airplane mode. The Court finds, therefore, that CBPO Beard's search of Defendant's iPhone violated CBP's border-search procedure.

While the Government understandably declines to concede this point outright, it nonetheless argues against suppression, contending that Officer Beard made a reasonable mistake of fact. *See Illinois v. Rodriguez*, 497 U.S. 177, 183–86 (1990) (warrantless search and seizure permissible if officers reasonably—but erroneously—believed they had been given permission by a resident to enter the premises). But, in the Court's view, the "ease" with which an iPhone can be placed in or out of airplane mode cuts against, rather than for, CBP. *United States v. Evans*, 782 F. App'x 340 (6th Cir. 2019), does not convince the undersigned otherwise.

In *Evans*, a police officer, hoping to find evidence of drug-trafficking activity once a search warrant was secured, attempted to put a cell phone belonging to an overdosed suspect in airplane mode. *Id.* at 341. In the course of doing so, familiar with his own Google Android rather than the suspect's Apple iPhone, the officer saw thumbnail

images of child pornography in the iPhone's camera mode and photo application before he managed to successfully activate airplane mode. *Id.* at 342. The district court denied the motion to suppress filed by overdosed suspect-turned defendant, because the police officer did not intend to unlawfully search the iPhone and because the child pornography would have been inevitably discovered after a search warrant was obtained in connection with the drug-trafficking activity. *Id.* at 343. The Sixth Circuit, in an unpublished opinion, vacated the district court's judgment and remanded the case. The officer's subjective intent was irrelevant, and thus the district court had applied the wrong Fourth Amendment standard. *Id.* at 343–44. Plus, the record was not developed enough for the district court to properly rule on inevitable discovery or the good-faith exception to the exclusionary rule. *Id.* at 344–45. In a footnote, however, the Sixth Circuit suggested, vis-à-vis the Supreme Court's "longstanding doctrine 'that searches and seizures based on mistake of fact can be reasonable[,]'" that the officer only "glimpsed" the child pornography "because he made a mistake—swiping left was not, as he believed, a way to access the settings application and enable airplane mode." *Id.* at 344 n.2.

In contrast to *Evans*, the record before this Court is very well-developed. CBP policy regarding the necessity to put a cellular phone in airplane mode before any search—whether manual or forensic—is clear. It is clear on paper and unequivocally understood by each officer who testified. To call CBPO Beard's own failure a "reasonable" mistake would undercut the policy, which, in the Government's words, is consistent with *Riley* because "CBP's border-search authority does not extend to searches of remotely stored information." (Doc. 37 at PageID 142.) *See United States*

v. Anderson, No. 4:07cr0023, 2007 WL 4732033, at *6 (officer's own clerical error cannot support "mistake of fact" argument).

The Government alternatively argues against suppression under the inevitable discovery exception to the exclusionary rule. *See Nix v. Williams*, 467 U.S. 431 (1984). But the record fails to support this theory.

CBPO Beard searched Defendant's iPhone during the brief time period while other officers were deciding whether Defendant's arrest record would trigger an NTA before an immigration judge. He searched *only* Google Photos on Defendant's iPhone and stopped when he found a *single* video of child pornography. He immediately turned the cell phone over to CBPO Mengel, who would not otherwise have searched it. According to Agent Wallace, Google Photos uses cloud storage for videos and Defendant's iPhone was accessing the cloud at the time of the search. Further, Wallace, the Government's forensic expert, could not confirm that the video viewed by Beard was resident on Defendant's iPhone. CPBO Beard's search, therefore, was unlawful.

Based on Agent Wallace's testimony, multiple images of child pornography were resident on Defendant's iPhone at the time of CBPO Beard's search. But there is no evidence to allow the Court to conclude that Beard inevitably would have found them. He did not testify that he would have searched the phone beyond Google Photos. He testified only that he viewed a single video of what he believed was child pornography and stopped. That Beard *could* have found additional child pornography is not the legal standard. Rather, the "burden of proof is on the government to establish that the tainted

evidence *would* have been discovered by lawful means." *United States v. Alexander*, 540 F.3d 494, 502 (6th Cir. 2008) (cleaned up) (emphasis added).

United States v. Chapman-Sexton, 758 F. App'x 437 (6th Cir. 2018), cited by the Government, is distinguishable. There the Sixth Circuit found that even though law enforcement had improperly searched a flash drive and found evidence of child pornography, an independent investigation by the defendant's probation officer also would have prompted a search of the flash drive. *Id.* at 440–42. *United States v. Galaviz*, 645 F.3d 347 (6th Cir. 2011), is likewise distinguishable. There the defendant was convicted of being a felon in possession of a firearm. The Sixth Circuit concluded it need not determine whether an officer improperly detained the defendant in his residence, because the gun in question was discovered in plain view in the defendant's vehicle by different officers called for backup. *Id.* at 352–54.

The inevitable discovery exception applies when evidence "discovered during an illegal search would have been discovered during a later legal search and the second search inevitably would have occurred in the absence of the first." *Chapman-Sexton*, 758 F. App'x at 441 (quoting *United States v. Keszthelyi*, 308 F.3d 557, 574 (6th Cir. 2002)). Yet there is no evidence that there inevitably would have been a "later" legal search. CBPO Mengel and Agent Melvin (and, obviously, Agent Wallace) were prompted to conduct their "later" searches based solely on CBPO Beard's illegal one. No other conclusion can follow from the testimony. Thus, this exception to the exclusionary rule is inapplicable.

The Court must now consider, actually as opposed to theoretically, whether good faith saves this search. It does not.

"We have repeatedly rejected the argument that exclusion is a necessary consequence of a Fourth Amendment violation. *Herring v. United States*, 555 U.S. 135, 141 (2009) (collecting cases). "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.* at 144. "[T]he exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct[.]" *Id.*

CBPO Beard's conduct was not deliberate, but it was in reckless disregard of the border-search policy. He failure to "ensure" that Defendant's iPhone was in airplane mode, knowing this was his obligation *and* knowing why. Every other officer and agent automatically presumed he followed the policy mandate before conducting their searches. The Government urges that this conduct "was no so objectively culpable to require exclusion." (Doc. 44 at PageID 157). Yet to hold otherwise would invite non-compliance with a bright-line requirement put in place by the CBP to comply with Supreme Court precedent.

This Court is all too aware that "our nation has classified child pornography as contraband for good reason." *Touset*, 890 F.3d at 1236. "The possession of child pornography 'harms and debases the most defenseless of our citizens,' in profound and lasting ways." *Id.* (quoting *United States v. Williams*, 553 U.S. 285, 307 (2008)). "The harm that victims suffer during the production of child pornography [for which Defendant Laynes is indicted] 'is exacerbated by the[ ] circulation' of 'a permanent record of the child['s] participation." *Id.* (quoting *New York v. Ferber*, 458 U.S. 747, 759 (1982)). Still,

under the circumstances of this case, the Court concludes that deterrence will serve its proper purpose.

III. CONCLUSION

Based on the foregoing reasons, Defendant's Motion to Suppress Evidence (Doc. 33), as supplemented (Docs. 36, 43) is hereby **GRANTED**. CBPO Beard's preliminary manual search of Defendant Laynes's iPhone violated the Fourth Amendment, and thus the video of child pornography that he viewed in the Google Photos application is suppressed. Additionally, all subsequent evidence of child pornography found on Defendant Laynes's iPhone is suppressed as the fruit of the poisonous tree. *See Wong Sun v. United States*, 371 U.S. 471 (1963).

IT IS SO ORDERED.

/s/ Michael R. Barrett
Michael R. Barrett, Judge
United States District Court